1. A system for providing secure access to secure information comprising:

a token in the possession of the token generator, where the token itself is random and non-predictable and contains no information but is used for the sole purpose of synchronization of the token processor and the token generator;

a token generator containing a transmitter used to pass the said token to a token processor;

a token processor having a reader for said token;

a token processor having the ability to generate a secure key to be used in the token generator to decipher an encrypted data sequence;

a token processor which has the ability to generate an encrypted data sequence based upon the secure key;

a token processor containing a transmitter used to pass the said secure key back to the token generator;

a token processor which has the ability to pass the encrypted data sequence for deciphering by the token generator;

a token generator which has the ability to receive the key from the token processor;

a token generator which has the ability to process the combination of the token and the key received from the token processor in order to decipher an encrypted data sequence;

2. A system as claimed in claim 1 wherein the said key is itself time-varying and non-predictable. The said key should be derived from the said token, though it is not solely

dependent on it, whether the said token is time varying or constant.

3. A system as claimed in claim 1 wherein the algorithm used in the token processor to generate the encrypted data sequence is embedded inside the token processor itself, and the algorithm used in the token generator to decipher the encrypted data sequence is embedded inside the token generator itself. The algorithms used in token generator and the token processor must match each other.

4 ~~5~~. A system as claimed in claim 1 wherein the said token can or cannot be modified by outside influences.

5 ~~6~~. A system as claimed in claim 1 wherein the said key can or cannot be modified by outside influences.

6 ~~7~~. A system as claimed in claim 1 wherein the algorithm used inside the token processor to generate the encrypted data sequence can or cannot be modified by outside influences.

7 ~~8~~. A system as claimed in claim 1 wherein the algorithm used inside the token generator to decipher the encrypted data sequence can or cannot be modified by outside influences.

FIELD OF THE INVENTION

This invention relates to techniques for controlling access to electronic information or other resources and more particularly to a method and apparatus for securely controlling access to such resources by use of a relatively simple token which defines a unique security key. This invention is especially useful in applications where the algorithm of generation of the said security key cannot be changed or modified over time while security of the data access must be maintained.

BACKGROUND OF THE INVENTION

There are many applications where information resources, must be shared between multiple users while these mentioned information resources should be protected from unauthorized access. Examples of such applications include various copyright protection titles (music CD, DVD, etc.), personal identification cards (bank cards, smart cards, medical cards, etc.). All those databases share one unique quality. Their security algorithm can be defined / programmed once when card is being issued and it is very difficult to modify / reset the algorithm later, when the title is sold / distributed. The information contained in those databases should be protected from unauthorized access while it should be easily shared between an unlimited number of authorized users. One can easily imagine a requirement for CDs to be played on any CD player while no useful data should be available for unauthorized copying. Similar to that bank cards should be accepted by all teller machines, while their data should not be available for fraud and/or theft purposes.

Usually an authorization of use of such resources is guaranteed by using an appropriate security key (PIN). This is not a preferred way of data exchange in copyright applications. It is not practical to expect consumers to memorize and enter their PINs for their CDs as a requirement for use. It is not beneficial to assign PINs for CDs as those PINs cannot be modified over time as well as they can be compromised. And finally, those PINs are not going to protect the copyrighted content from malicious misuse by one of its own authorized customers who would like to make an unauthorized copy.

Thus, for certain classes of applications it is important to deliver secure information to the end user in an encrypted form, which while providing the necessary service, shall never expose the real data in its original form and thus prevent said data from being deciphered.

Prior art systems usually use a password approach when transmitting secured data over a public network. An authorized user's request for the data should be verified for validity by confirming the transmitted secure PIN or password. This potentially compromises the system security and makes it vulnerable to an unauthorized user who can obtain the encryption algorithm by monitoring small known pieces of data transmission obtained from any unrelated source. Using therefore mentioned example of the music CD, an unauthorized individual may be able to learn the security PIN and eventually decipher the data by obtaining a small piece of deciphered musical data. This deciphered data can be used as a key for back calculating the PIN. Subsequently, all data available on the CD will be compromised. Significant problems for this kind of application arise from the fact that the PIN cannot be modified over time because it is stored on the said CD at the time of its manufacturing.

The fact that the PIN cannot be modified and should be assigned once and forever - for the lifetime of the music CD, makes it very susceptible to an unauthorized user attack, especially since there are plenty of music fragments available in public in deciphered format.

Password systems use only one of the three possible factors which are available to provide a secure system, namely, something the user knows. The other two factors are something an authorized individual has, for example a token, and something the individual is, for example a bio-characteristic. More secure resource access systems involve at least two of the factors, normally something the individual knows and something the individual has in his possession. However, it has been found that tokens containing a secret (i.e. non-observable) static code value are also subject to surreptitious detection by, for example, the monitoring of a line over which such value is being transmitted. It is also possible that the token could be "borrowed", read by a suitable device to obtain the secret user code and then returned before the owner realizes it is missing. In either event, the token containing the code could be recreated and used for some period of time to gain access to sensitive information within a database or to other information resources without detection. Therefore, improved "smart" tokens, such as those disclosed in U.S. Pat. Nos. 5,657,388; 5,023,908, and 4,720,860 and various related patents have varied the values stored in the token, or at least the value outputted from the token, in accordance with some algorithm which causes the values to vary in a non-predictable way with time so as to provide unique one-time codes.

Such devices have provided significantly enhanced security for secret access codes. They significantly enhanced security for the data processing system, database or other information resource with which such devices are being utilized. However a "smart" smart card (which for purposes of this application is defined as a card having data processing capability) has been required to use such systems. Those cards are required to have significant processing capabilities and are expensive to manufacture. It seems to be obvious and hardly needs any additional prove that music CDs, for example, can't have this "smart" functionality because of the associated cost.

A need therefore exists for an improved secure access technique which provides the advantages of one-time code and the possibility of two factor security while permitting the use of inexpensive and relatively small specialized hardware for token generation and processing.

SUMMARY OF THE INVENTION

In accordance with the teachings of this invention, a "dumb token" is generated by the token generator which is utilized to synchronize the token generator and the token processor, such a token being created in machine readable form. The token is transmitted from the token generator to the token processor. The token processor is utilized to generate, both from the token it received from the token generator and an internally created random offset, a non-repetitive, non-predictable key. The key is transmitted back to token generator. Now both the token generator and the token processor possess copies of the token and the key. The token processor utilizes its embedded algorithm in conjunction with the combination of the token and the key, to create a time varying encryption sequence, which is used in turn to encrypt the sensitive data. The encrypted data is then transmitted from the token processor to the token generator. The token generator utilizes its embedded algorithm in conjunction with the combination of the token and the key, to create a time varying decryption sequence, which is used in turn to decipher the sensitive data received from the token processor.

The transmitters and receivers at the token processor and token generator may be modems interconnected by a telephone line network interface or the transmitter and receiver may be elements of a radio/cellular network. Other communication techniques between processors known in the art may also be utilized.

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments of the invention as illustrated in the accompanying drawings.

IN THE DRAWINGS

FIG. 1 is a semi-schematic diagram of hardware for practicing the teachings of this invention.

FIG. 2 is a flow diagram for the operation of the system of FIG. 1 in accordance with practicing various embodiments of the invention.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates the two basic components of a system utilized in practicing the teachings of this invention, these components being a token generator 1-00, and a token processor 2-00. Token is preferably a "dumb" token, which contains no information and is used for the sole purpose of synchronizing the mentioned embodiments the said token processor 1-00 and the token generator 2-00. The token is generated by the first random number generator 1-02 and then in the simplest case is passed over to the token transmitter 1-04. However, for various embodiments of the invention it may also be desirable to pass it to the decryption engine 1-10. The token transmitted by the token generator 1-04 is received by the token receiver 2-02, and then subsequently passed to the key generator 2-06. As it will be discussed in greater detail later, for some embodiments, the key is being generated in key generator 2-06 not only based on the random token, but also may be affected by the output of the second random number generator 2-04. The second random number generator 2-04 allows for removing deterministic relationship between the token and the key. This improves the overall security of the system. The key generated by the key generator 2-06 is fed back to the token generator 1-00 via the key transmitter 2-08 and key receiver 1-06. The key generated by the key generator 2-06 is used for data encryption in encryption engine 2-10. Both the data, represented in an "open" format, from the data storage 2-14 and the key from the key generator 2-06 are fed into the encryption engine 2-10 simultaneously. Encrypted data is passed to the token generator 1-00 via the data transmitter 2-12. For some embodiments the said encryption engine 2-10 can perform the encryption operation not only based on the key, but taking into account the token received by the token receiver 2-02. Decryption engine 1-10 located inside the token generator 1-00 performs decryption of the data passed from the data transmitter 2-12 via the data receiver 1-08. Decryption can be performed either solely based on the key received by the key receiver 1-06 or, as it will be discussed later, based on both the key and the token, which comes directly from the first random number generator 1-02. The output of the decryption engine 1-10 is fed into the backend interface 1-12, from where the data can be consumed by an authorized user and/or application.

Referring now to FIG. 2, the first step in the using of the system is for the user to start 3-00 the Token Generator so it will generate 3-02 a dumb token. This might happen as a result, for example, of Token Processor being directly engaged with the Token

Generator. Upon being initialized, the Token Generator generates the token, 3-02 and then transmits it towards the Token Processor, using the token transmitter 3-04. After the token was sent, the Token Generator enters an endless loop, waiting for the decryption key to be received, 3-08. This loop, 3-08 might be terminated by a watch dog timer or utilizing any other known means suitable to prevent a lock-up condition. While Token Generator is awaiting the key to be received, the Token Processor waits in an initial endless loop, 4-04, for the said token transmitted by the token transmitter, 3-04 to be received by the token receiver, 4-02. Upon receiving a valid token, the token processor generates the key in the key generator, 4-08. This process of key generation may be solely dependent on the token received, but it can also be based on an internally generated random offset, 4-06 or it might depend on both of those said values, the token and the random offset. After the key is generated, 4-08, it is transmitted by the key transmitter, 4-10 back to the token generator, where the valid key is identified by the key receiver, 3-06. After the key is transmitted, 4-10, the token processor utilizes it in conjunction with an algorithm defined for the token processor to generate an encryption sequence, 4-12. When the encryption sequence is ready, the data can be picked up from the data storage, 4-14 in order to be encrypted, 4-16 and subsequently transmitted to the token generator using the data transmitter, 4-18. Token generator upon receiving the valid key, 3-06 exits the endless loop it entered after the token was transmitted and generates the decryption sequence, 3-10 utilizing an algorithm defined for the token generator to generate a decryption sequence. When the decryption sequence is generated, it can be used for decryption of the data, 3-14 received by the data receiver. The user at its own discretion can further utilize the decrypted data.

Both the encryption and decryption sequences can be synchronously modified during the data transmitting in order to enhance communication security. In the latter case the decision to change the encryption sequence, 4-20 is made in token processor at random or repetitive time intervals. The token generator either changes its decryption sequence, 3-16 based on a control sequence embedded in the data stream or repetitively based on the predefined time intervals.

Thus, while the invention has been particularly shown and described above with reference to preferred embodiments, the foregoing and other changes in form and detail may be made therein by one skilled in the art without departing from the spirit and scope of the invention.